SAGRADO
Universidad del Sagrado Corazón

# Procedimiento para la Respuesta a un Incidente de Seguridad de Sistema de Información

Efectivo: 2019.07.01

## Propósito

Sagrado (también conocido como "Universidad") establece este Procedimiento que describe los procesos que se deben seguir cuando se descubre que ha ocurrido un incidente de seguridad informática que involucra un sistema de información computarizada operado por la Universidad, sus profesores regulares y parciales, estudiantes, empleados administrativos y de propuestas, consultores, proveedores u otros que operan tales sistemas en nombre de Sagrado. También describe los procedimientos que se deben seguir cuando se acceda inapropiadamente a la Información Restricta o Confidencial que reside en cualquier dispositivo informático o de almacenamiento de información, ya sea que dicho dispositivo sea propiedad de Sagrado o no. Este procedimiento describe los procesos para la toma de decisiones con respecto a las acciones de emergencia que se tomarán para proteger los recursos de información de Sagrado contra el acceso accidental o intencional no autorizado, la divulgación o posible daño de dicha información.

El propósito de la respuesta al incidente de seguridad de la información es:

- Mitigar los efectos causados por dicho incidente;
- Proteger los recursos de tecnología de información de la Universidad evitando un futuro acceso no autorizado, prevenir el uso o daño de dicha tecnología;
- Garantizar que Sagrado cumpla con todas sus obligaciones bajo el procedimiento de la Universidad, y las leyes y regulaciones federales y estatales con respecto a dicho incidente;
- Asegurar la protección, confidencialidad, integridad y disponibilidad de información sensitiva incluyendo información electrónica protegida;
- Asegurar la prevención de cualquier actividad inusual y/o anormal que envuelve recursos tecnológicos de información;
- Asegurar la protección de los sistemas de información de la Universidad con el fin de mitigar vulnerabilidades, riesgos y amenazas.

## Aplicabilidad

Este Procedimiento aplica a todos los estudiantes universitarios, facultad regular y parcial, empleados administrativos y de propuestas y a otros ("usuarios") con acceso y uso de los recursos de tecnología e información ("IT") de Sagrado.

## Definiciones

*Sistema de computación*. Cualquier aplicación, o sistema de información, que directa o indirectamente trate o respalde la Misión de la Universidad de enseñanza, aprendizaje e investigación, información financiera, administrativa o de otra índole que es una parte integral de la gestión de la Universidad.

*Información confidencial*. Como se define en la Política de Seguridad de la Información.

*Incidente de seguridad de información electrónica*. Cualquier evento adverso real o sospechado en relación con la seguridad de los sistemas informáticos, redes informáticas, información restringida electrónica, información confidencial electrónica. Ejemplos de incidentes incluyen:

- Intentos (fallidos o exitosos) de obtener acceso no autorizado a un sistema o sus datos;
- Robo u otra pérdida de una computadora portátil, computadora de escritorio, asistente digital personal o agenda electrónica (PDA) u otro dispositivo que contenga información restringida o confidencial, ya sea que dicho dispositivo sea o no propiedad de Sagrado;
- Interrupción no deseada o denegación de servicio;
- El uso no autorizado de un sistema para el procesamiento o almacenamiento de datos;
- Cambios en los componentes físicos ("hardware") del sistema, el soporte lógico inalterable ("firmware") o las características de los programas informáticos ("software") sin el conocimiento, la instrucción o el consentimiento del propietario.

*Incidente de seguridad de la información*. Robo real o presunto, pérdida u otro acceso inapropiado de información electrónica tales como correos electrónicos, computadoras, redes de conexión.

*Incidente de seguridad de la información no electrónico*. Robo real o presunto, pérdida u otro acceso inapropiado de contenido físico, como documentos y archivos impresos.

*Información restricta*. Como se define en la Política de Seguridad de la Información.

### Notificación

Cualquier usuario que tenga conocimiento de un incidente de seguridad de la información debe:

- Apagar la computadora o desconectar el sistema y el equipo que ha estado expuesto o comprometido de la red de Sagrado;
- Evitar hacer actualizaciones u otras modificaciones al software, datos o equipos involucrados o que se sospeche que están involucrados en un Incidente de Seguridad de la Información hasta tanto la Oficina de Información y Tecnología Integrada (ITI) haya completado su investigación y autorice dicha actividad;
- Contactar al Principal Oficial de Información (CIO) al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

## V. Investigación

Cuando se informa un incidente de seguridad de la información, el CIO procederá de la siguiente manera:

1. Investigar el incidente de seguridad de la información y, de entenderlo apropiado, restringir el acceso u operaciones del sistema de información para proteger posibles divulgaciones de información no autorizadas, minimizar el impacto del incidente de seguridad de la información en la Universidad, o completar la investigación. El CIO puede convocar de forma preliminar a un grupo de trabajo para esclarecer los hechos compuesto por personal relevante tanto gerencial como técnico.

2. Si el CIO concluye que las leyes o reglamentaciones federales o estatales aplicables pueden haber sido violadas, el CIO notificará al Asesor Legal General que notificará a las agencias encargadas de hacer cumplir la ley, si corresponde.

3. Si el CIO concluye que existe la posibilidad de acceso no autorizado a información Restricta o Confidencial u otra información sensitiva, el CIO convocará un Equipo de Respuesta a Incidentes de Seguridad de la Información (ISIRT - “Information Security Incident Response Team”).

4. Si corresponde, el CIO notificará a las oficinas de los funcionarios autorizados académicos o del personal con responsabilidad sobre las áreas afectadas por el incidente de seguridad de la información.

5. Si el CIO determina que un empleado puede no haber llevado a cabo sus tareas asignadas según las instrucciones o de acuerdo con las normas y políticas de la Universidad, el CIO notificará al gerente del empleado y al Vice-presidente de

Desarrollo Organizacional y Recursos Humanos para que investigue y determine la acción correctiva o disciplinaria apropiada, si corresponde.

### Equipo de Respuesta al Incidente de Seguridad de la Información

Dependiendo de la naturaleza del incidente de seguridad de la información, el CIO y en consulta con el Asesor Legal General convocará un Equipo de Respuesta a Incidentes de Seguridad de la Información (ISIRT) para desarrollar un Plan de Respuesta a Incidentes de Seguridad de la Información (Plan ISIRT).

El ISIRT desarrollará y ejecutará planes de comunicación y otros planes de acción para garantizar que:

- Se tomen las medidas adecuadas en un tiempo oportuno, incluida la notificación, informes y otras comunicaciones del incidente de seguridad de la información, según lo exija la ley o se considere apropiado.
- Se realicen los informes de progreso apropiados sobre el incidente de seguridad de la información y la ejecución del Plan ISIRT.

- Como parte de su responsabilidad, el ISIRT asegurará que las decisiones operativas importantes se eleven a los niveles apropiados para proteger los intereses fundamentales de la Universidad y otros afectados por el incidente.

El CIO también será responsable de documentar las deliberaciones y decisiones de la ISIRT, así como todas las acciones tomadas conforme con los análisis de dicho equipo.

### Preparación del Informe

El CIO será responsable de redactar un informe final sobre el incidente que resuma la investigación, los hallazgos, el Plan ISIRT y su ejecución, y recomendaciones para mejorar las prácticas y controles relacionados a la seguridad de la información

### Informar el Uso Indebido de este Procedimiento

Los usuarios tienen la responsabilidad de reportar sospechas de incidentes de uso indebido de este Procedimiento para responder a incidentes de sistemas de información incluyendo, pero sin limitarse a, sospechas de actividades ilícitas o impropias al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

Inspección y monitoreo la información y los recursos de IT pueden ser necesarios para cumplir con este Procedimiento, realizar investigaciones o auditorías, garantizar la seguridad de una persona o de la Universidad, cumplir con la ley o garantizar el

funcionamiento adecuado de los recursos de IT. Solo el CIO (o designado) puede autorizar esta inspección y monitoreo.

Se espera que los usuarios de los recursos de IT cooperen con cualquier investigación de abuso de Políticas y Procedimientos. La falta de cooperación puede ser motivo de cancelación de privilegios de acceso u otras medidas disciplinarias.

### Consultas sobre este Procedimiento

Las consultas sobre el alcance y la interpretación y de este Procedimiento deben dirigirse al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

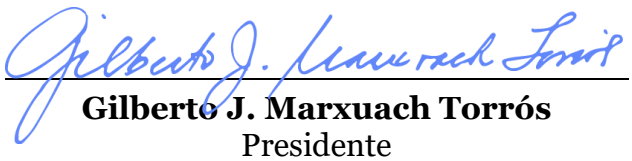
### Denuncias de Violaciones al Procedimiento

Las violaciones a este Procedimiento o las consultas sobre el alcance y la interpretación de este Procedimiento deben dirigirse al Asesor Jurídico al 787.728.1515, ext. 1221, o por correo electrónico a cameliac.fernandez@sagrado.edu, o al Oficial de Cumplimiento e Integridad al 787.728.1515.

### Violaciones a este Procedimiento

La Universidad del Sagrado Corazón se reserva el derecho de interpretar este Procedimiento en su administración, implementación y aplicación. Cualquier violación de este Procedimiento por parte de un estudiante, profesorado o personal o cualquier otra persona puede resultar en una acción disciplinaria que puede incluir la expulsión de la Universidad (estudiantes) o la terminación de la relación laboral (personal docente y administrativo) u otras acciones legales apropiadas.

Si existe alguna ambigüedad en cualquier disposición de este Procedimiento, la Universidad se reserva la discreción de interpretarla de acuerdo con el propósito para el cual fue establecida, el impacto en las operaciones de la Universidad y la buena fe, a menos que cualquier ley establezca lo contrario.



**Gilberto J. Marxuach Torrós**
Presidente